Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in The U.S. DISTRICT COURT at Seattle, Washington.

February 9 20 06

BRUCE RIFKIN, Clerk

By H. Brent Zachary Deputy

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

CHRISTOPHER MAXWELL,

Defendant.

NO. CR06 0042P

INDICTMENT

06-CR-00042-INDI

The Grand Jury charges that:

COUNT 1

(Conspiracy to Intentionally Cause Damage to a Protected Computer and to Commit Computer Fraud)

A. The Offense

1. Beginning at a time uncertain, but in or about July, 2004, and continuing until on or about July 7, 2005, within the Western District of Washington and elsewhere, CHRISTOPHER MAXWELL did knowingly and willfully conspire, combine, confederate, and agree together with others, known and unknown to the Grand Jury, to commit offenses against the United States, to wit: intentionally causing damage to a protected computer, in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(a)(5)(B)(ii), 1030(b), and 1030(c)(4)(A), and computer fraud, in violation of Title 18, United States Code, Sections 1030(a)(4), 1030(b), and 1030(c)(3)(A), and committed acts in furtherance of that conspiracy.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

B. Background

At all times material herein,

2. CHRISTOPHER MAXWELL was a resident of Vacaville, California.

3. Northwest Hospital was a 187 bed, community-based, not-for-profit hospital, located in Seattle, Washington that owns, operates and daily relies upon computers used in interstate and foreign commerce and communication.

Adware

4. Adware is computer software that displays advertisements. Adware companies make money by selling advertising exposure for products or services to the company or individual that is marketing those products or services. To enhance the value of their service - displaying advertisements - adware companies seek to increase the number of computers that run their software. One strategy employed involves "affiliate marketing" programs, whereby the adware companies offer to pay commissions to their "affiliates" based upon the number of installs made of the adware. Each affiliate has a unique identification number or code that is included in the installation software. When the adware software is installed, it initiates a transmission, over the Internet, of that unique identifier back to the adware company. The adware company then tallies up the number of installations by each affiliate and periodically pays the affiliate his or her commission, usually through an online payment service such as Paypal, by checks mailed to the affiliate, or through direct bank deposits.

5. Adware is usually installed on an Internet user's computer only upon notice or if the user performs some affirmative action, like downloading other software that is attractive to the user, and with which the adware has been "bundled" or combined. Examples include peer-to-peer file sharing programs, free screen savers, and desktop wallpaper programs. The adware can also be "silently" installed, however, without user interaction and without displaying a consent form or end-user license agreement. Adware companies' affiliate programs rely on the affiliate to obtain the end-users'

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

consent for installation of the adware, typically by appending notification to the user license agreement provided by the software with which the adware is bundled.

Internet Rely Chat and IRC Botnets

6. Internet Relay Chat ("IRC") is a text based communications protocol for person-to-person communication ("chat") between computers on the Internet. IRC requires one or more servers and one or more clients. A client is a computer, or software running on that computer, that is used by a person to chat via IRC. A server is a computer, or software running on that computer, that manages connections between the many clients and relays messages to the appropriate recipients. IRC offers the ability to have private conversations with only select clients or public conversations with only select clients or public conversations with multiple clients. IRC uses "channels" to determine which users are parties to which conversations. IRC supports the use of passwords, or "keys" to limit access to servers and channels. IRC also provides an administrative level of access, known as an "operator," at the channel and server level to provide configuration and policy enforcement. IRC channels have names, that uniquely identify them, and "topics," that usually describe the conversation happening on the channel.

7. An IRC network is a collection of computers communicating with each other via IRC. Generally, an IRC network includes numerous clients (between a few dozen and tens of thousands) and one or several servers (most small networks can operate with only one server, but many have several for performance and availability reasons). Servers are generally always available, while clients connect and disconnect at various times.

8. An IRC robot, or "bot," is a program running as an IRC client that responds autonomously to commands sent to it by the IRC server; it can thus receive commands, perform functions, and provide information back to the IRC server without human interaction at the client level. A computer infected with a malicious IRC bot

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

and connected to an IRC server is often also referred to as a "bot" or "zombie" or "drone."

9. An IRC botnet is an IRC network composed primarily of IRC bots, rather than human clients. The bot clients (i.e., computers infected with an IRC bot) are configured to connect to an IRC channel and "wait" there for further commands. The botnet operator or controller (i.e., a human using an IRC client program) issues those commands by connecting to the IRC server, on the appropriate channel, and then issuing the commands. Most malicious bot programs are also capable of interpreting an IRC channel topic as a command. This allows the owner/operator of the botnet to configure a persistent command, which will be received and executed by every bot as it connects to the channel. This allows the botnet to operate without constant interaction by the owner/operator.

10. Malicious bots are installed on computers without the knowledge or consent of the computers' owners. The creator of the botnet typically does this by using a computer or computers to electronically scan or search, over the Internet, for computers with particular vulnerabilities or security weaknesses. He or she then uses an "exploit" or computer code written to take advantage of those vulnerabilities or weaknesses to compromise or "hack" the victim computer. Once the victim computer has been hacked, the computer can be infected and made a bot through the installation of malicious bot code. The bot code program connects to the appropriate IRC channel, where it will receive commands from the owner/operator of the botnet.

11. Most malicious bot code includes code that enables the infected bot computer to also scan the Internet for, and compromise other computers, and infect these additional computers with the malicious bot code. By this means, the botnet can continually spread and grow. Depending on the intended use, botnets can range in size from fewer than one hundred computers to tens of thousands of computers. A botnet will grow and shrink in size as new computers are infected, or existing, infected computers are cleaned, shutdown, or removed from the Internet.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

12. The process of scanning for vulnerable computers to add to the botnet is often done in a random, inefficient manner. While the process is generally successful, it inevitably generates large amounts of network traffic, particularly within local networks. The increase in network traffic can be enough to completely interrupt and disable normal network communications. The network client computers are unable to perform their intended functions, and may require significant repairs in order to resume those normal functions.

13. Creators, owners and operators of botnets can locate their botnet servers or channels on server computers that they own, or that they have leased from others. IRC server software can also be installed on compromised or hacked computers, without the knowledge or permission of the owners of those computers. Botnet owners and operators can also move their illicit botnet servers and channels from server to server, to avoid or hamper detection.

Other Computer and Internet Terminology

14. Domain Name Service ("DNS") is an Internet resource for converting alphanumeric names into Internet Protocol ("IP") addresses. Computers on the Internet are assigned 32-bit IP addresses, that are represented by four numbers, each from 0 to 255, separated by periods. These numbers, ranging from four to twelve digits in length (0.0.0.0 through 255.255.255.255) are often difficult for people to remember. DNS provides several features, including the ability to refer to Internet addresses by easy-to-remember names rather than difficult-to-remember numbers. DNS provides other benefits, including the ability to change the underlying IP address while preserving the availability of the resource. Users can continue to request the resource by alphanumeric name, and DNS will resolve the name to the new IP address. DNS also provides the ability to have a name resolve to multiple IP addresses, for performance and load-balancing reasons or to provide some protection against the failure of a single IP address or computer.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

15. Domain names are organized hierarchically and read right-to-left. The right-most component is the "top level domain." This includes the ".com," ".gov," ".mil," and ".edu" domains as well as many others. Top level domains are owned and managed by the Internet sanctioning organizations. The second part of the domain name is owned by the registrant who first registered the name with the sanctioning organizations. It is common to refer to a registered domain and top-level domain combination as a "domain name." Examples include "cybercrime.gov" and "fbi.gov." Domain name owners can then create sub-domains to provide addresses to resources they own or control. For example, the DNS sub-domain "www" is generally used to denote an organization's web server, so "www.fbi.gov" would, and does, both denote and lead to the FBI's web site. Another sub-domain, "seattle.fbi.gov," leads to the Seattle office's web site.

16. Numerous Internet companies offer free sub-domains to their customers. These companies typically have a collection of domain names that they have registered, and allow their customers to create sub-domains of the domain names and control the IP addresses to which those sub-domains resolve. Often, these sub-domains can be created and configured without divulging much, if any, true information about the customer.

17. DNS sub-domains are useful in the creation and maintenance of IRC botnets because they provide a convenient means to ensure that bots can continue to locate the IRC server even as it moves from computer to computer. The sub-domain name is generally programmed into the bot so that each time it tries to connect, it resolves the sub-domain to one or more IP addresses, and then tries to connect. If the botnet owner needs to move the IRC server, he or she simply moves the server, and then updates the DNS sub-domain record to point to the new server's IP address.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

C. Object and Purpose of the Conspiracy

18. The object of the conspiracy was to profit unjustly by creating and using one or more IRC botnets remotely and surreptitiously to install adware or other unauthorized programs on thousands of compromised computers, without the knowledge or consent of the computers' owners, and thereby obtain thousands of dollars in commission payments from adware companies for those installations.

D. Manner and Means of the Conspiracy

19. It was part of the conspiracy that CHRISTOPHER MAXWELL and his coconspirators intended to and did create an Internet Relay Chat ("IRC") network; that is, a collection of computers communicating with each other over the Internet via IRC. The IRC network created by CHRISTOPHER MAXWELL and his coconspirators included at times more than thirteen thousand client computers used in interstate communications, and one or more server computers.

20. It was further part of the conspiracy that CHRISTOPHER MAXWELL and his coconspirators added client computers to their IRC network by remotely compromising or "hacking" into computers that were owned and operated by others, without the knowledge or consent of the computers' owners.

21. It was further part of the conspiracy that CHRISTOPHER MAXWELL and his coconspirators, after having remotely compromised computers, remotely installed on those compromised computers a malicious IRC client program, with the intended result that the IRC clients were programmed to respond autonomously to commands sent to them via the IRC servers created and controlled by CHRISTOPHER MAXWELL and his coconspirators. The network of client computers thus became a network of "robot" or "bot" computers, also know as a "botnet," the client members of which were subject to command and control through the IRC servers created and controlled by CHRISTOPHER MAXWELL and his coconspirators.

22. It was further part of the conspiracy that the malicious code with which CHRISTOPHER MAXWELL and his coconspirators infected the individual IRC bots

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

enabled and commanded those bots repeatedly to seek out, or scan for and compromise other computers, thereby contributing to the spreading of the botnet to new and previously uninfected computers. Voluminous network traffic generated by this scanning had the effect of simultaneously limiting or even preventing the compromised computers from functioning normally and properly in accordance with the intent and directives of their legitimate owners and operators.

23. It was further part of the conspiracy that CHRISTOPHER MAXWELL and his coconspirators used their botnet intentionally to cause and command compromised computers surreptitiously to install adware on computers used in interstate communications without the knowledge or consent of the computers' owners.

24. It was further part of the conspiracy that the compromised computers on which the botnet had installed adware would "register" those installations with adware companies, which would in turn generate profits by way of illicit commission payments to CHRISTOPHER MAXWELL and his coconspirators.

25. It was further part of the conspiracy that CHRISTOPHER MAXWELL and his coconspirators received commissions totaling approximately one-hundred thousand dollars, as a result of the surreptitious and unauthorized installation of adware by and through their botnets.

26. It was further part of the conspiracy that CHRISTOPHER MAXWELL and his coconspirators also hacked into computers that belonged to others for the purpose of using them as servers for their IRC botnet. MAXWELL and his coconspirators would accomplish this by using a variety of remote exploits to gain unauthorized access to remote computers, and then surreptitiously installing IRC server software on those computers without the knowledge or consent of those computers' owners. Because a high-powered computer was needed to perform the functions of an IRC Server, MAXWELL and his coconspirators often targeted high-powered computers that were part of institutional computer networks, including those of California State University, Northridge; the University of Michigan; and University of

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

California, Los Angeles. The surreptitious use of those compromised computers as illicit botnet IRC servers necessarily impaired and disrupted the normal functions and operations of the compromised computers.

27. It was further part of the conspiracy that CHRISTOPHER MAXWELL and his coconspirators would act intentionally to avoid detection and disruption of their illicit IRC servers by repeatedly moving the servers from one computer to another. When doing so, MAXWELL and his coconspirators would also change the Domain Name Service ("DNS") sub-domain record, which had been previously programmed into the bots, to "point to" or resolve to the new server's IP address. This change in the sub-domain record enabled the bots to find the relocated IRC server at its new location.

28. It was further part of the conspiracy that CHRISTOPHER MAXWELL and his coconspirators configured or commanded the bots that were part of their botnet to connect to a designated IRC channel on a specified IRC server, and to "wait" there for further commands. CHRISTOPHER MAXWELL and his coconspirators would, at their discretion, connect to the IRC channel and configure persistent commands that would be received and executed by every bot as it connected to the channel. This system would allow the botnet to operate continuously without constant interaction by CHRISTOPHER MAXWELL and his coconspirators.

29. It was further part of the conspiracy that CHRISTOPHER MAXWELL and his coconspirators intentionally caused damage - that is, impaired the integrity or availability of data, a program, a system, or information - in each instance in which they compromised a protected computer without the knowledge or consent of that computer's owner, whether the compromised computer was one that was made a bot or an IRC server for the botnet.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

E. Overt Acts

In furtherance of the conspiracy and to achieve the objects thereof, at least one of the coconspirators committed or caused to be committed, in the Western District of Washington, and elsewhere, at least one of the following overt acts, among others:

30. On or about July 16, 2004, CHRISTOPHER MAXWELL created a login account with DNSMadeEasy, a company that provides free sub-domain name accounts. CHRISTOPHER MAXWELL created the account "sasserpwn" using the email address "donttrip31337@cashette.com."

31. On a date uncertain, but between July 16, 2004, and January 9, 2005, CHRISTOPHER MAXWELL created two sub-domain name entries: "dust.page.us" and "test0r.server.us" and programmed these two names into the source code of the IRC bot program that MAXWELL and his coconspirators had created.

32. On a date uncertain, but between July 16, 2004, and January 9, 2005, CHRISTOPHER MAXWELL and his coconspirators used the name "dust.page.us" to direct compromised computers to a file transfer protocol ("FTP") server containing a copy of the malicious program, which compromised computers were directed to download and execute.

33. On a date uncertain, but between July 16, 2004, and January 9, 2005, CHRISTOPHER MAXWELL and his coconspirators used the name "test0r.server.us" to direct bot computers to the IRC server or servers MAXWELL and his coconspirators used to maintain and control the botnet.

34. On or about January 9, 2005, CHRISTOPHER MAXWELL and his coconspirators utilized the botnet that they had created and that they controlled knowingly and surreptitiously to install adware on a protected computer belonging to Northwest Hospital, without the knowledge or consent of Northwest Hospital, and as a result thereof furthered their intended computer fraud in an attempt to obtain profits in the form of illicit commission payments. The computer scanning activity and resultant increase in network traffic within the Northwest Hospital computer network associated

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

with those acts interrupted normal network computer communications of Northwest Hospital, with consequences to numerous hospital systems including, but not limited to, the hospital's surgical system, patient financial system, information management system, diagnostic imaging services, and laboratory services. The interruptions caused to Northwest Hospital's normal network communications also caused the modification or impairment, or potential modification or impairment of the medical diagnosis, treatment, or care of one or more of its patients, due to delays in providing information to physicians, delays in timely communicating diagnostic information, delays in processing laboratory test results, delays in scheduling surgery, and the temporary loss of critical computers in ICU hospital rooms. The financial costs to Northwest Hospital of responding to the botnet intrusion on or about January 9, 2005 have been initially estimated at $149,000.00.

35. On a date uncertain, but in or about March, 2005, CHRISTOPHER MAXWELL compromised the security of, and intruded upon a computer having the IP address **.**.*79.10 that was owned by The Planet, an Internet service provider located in Dallas, Texas, and leased to one of their customers. After gaining unauthorized access to the computer at The Planet, MAXWELL remotely and surreptitiously installed IRC server software on that computer to allow him to operate and control a botnet using that computer.

36. On or about March 16, 2005, CHRISTOPHER MAXWELL configured the sub-domain name "test0r.server.us" to direct traffic to the IP address of the compromised computer at The Planet.

37. By configuring the sub-domain name "test0r.server.us" to direct traffic to the IP address of the compromised computer at The Planet on or about March 16, 2005, MAXWELL caused computers infected with the IRC bot program to establish persistent communications with the IRC server, allowing him to issue commands to all connected bot computers via IRC.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

38. CHRISTOPHER MAXWELL and his coconspirators did, and caused to be done, the acts set forth in Count 2 of this Indictment, which is incorporated by reference and alleged as a separate overt act as if set forth in full herein.

All in violation of Title 18, United States Code, Section 371.

COUNT 2

(Intentionally Causing and Attempting to Cause Damage to a Protected Computer and Thereby Causing Loss in Excess of $5,000 and Modification or Potential Modification of Medical Treatment)

On or about January 9, 2005, within the Western District of Washington and elsewhere, CHRISTOPHER MAXWELL knowingly caused and attempted to cause the transmission of a program, information, code, and command, that is, malicious botnet source code, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to computers belonging to, and used in interstate commerce and communications by Northwest Hospital, in Seattle, Washington, and others, and by which conduct CHRISTOPHER MAXWELL caused an aggregate loss to Northwest Hospital of at least $5,000 in value during a one-year period, and by which conduct CHRISTOPHER MAXWELL caused the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(a)(5)(B)(ii), 1030(b), 1030(c)(4)(A), and 2.

FORFEITURE ALLEGATIONS

1. The allegations contained in Counts 1 and 2 of this Indictment are realleged and incorporated by reference for the purpose of alleging forfeiture to the United States of America of certain property in which the defendant has an interest.

2. Upon conviction of any of the offenses charged in Counts 1 and 2 of this Indictment, the defendant shall forfeit to the United States pursuant to Title 18, United

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

States Code, Section 982(a)(2)(B) any property constituting or derived from proceeds obtained directly or indirectly as a result of the said violations, including but not limited to the following:

a. All funds held in Paypal Account No. **********5225 , in the name of CHRISTOPHER MAXWELL;

b. All funds held in checking account No. ******0129 at Wells Fargo Bank, in the name of CHRISTOPHER MAXWELL;

c. All funds held in savings account No. ******9657 at Wells Fargo Bank, in the name of CHRISTOPHER MAXWELL.

A TRUE BILL:

DATED: 9 FEBRUARY 2006

Signature of Foreperson redacted pursuant to the policy of the Judicial Conference of the United States.

FOREPERSON

JOHN McKAY
United States Attorney

KATHRYN A. WARMA
Assistant United States Attorney

CARL BLACKSTONE
Assistant United States Attorney

RICHARD E. COHEN
Assistant United States Attorney

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970